CLAIMS

WE CLAIM:

1. A safety controller comprising:

a primary processing unit having a first processor communicating with a first memory holding a safety program requiring a first reliability of operation and a standard program requiring a second reliability of operation less than the first reliability of operation;

a second processor having a second processor independent from the primary processing unit and communicating with a second memory independent from the first memory and holding the safety program and not the standard program; and

a synchronization program executable by the primary and partner processing units to execute the standard program in the primary processing unit only and to execute the safety program in the primary and second processing units and to compare execution of the safety programs to enter a safety state when this execution differs.

2. The safety controller of claim 1 wherein the primary processing unit is in a first housing and the partner processing unit is in a second housing independent from the first housing and further including a communications bus communicating between the first and second housings to allow intercommunication between the primary and partner processing units.

3. The safety controller of claim 1 wherein the communication bus is a backplane and wherein the primary and partner processing units communicate through releasable electrical connectors on the backplane.

4. The safety controller of claim 1 wherein the communications bus is a serial communications network and wherein the primary and partner processing units communicate through releasable electrical connectors on the serial network.

5. The safety controller of claim 1 wherein the primary and partner processing units are in a single housing.

6. The safety controller of claim 1 wherein the first memory includes at least a portion that is lockable by hardware against writing.

7. The safety controller of claim 1 wherein the safety program executes to generate outputs to be used to control an external device and wherein the synchronization program compares execution of the safety program by comparing outputs generated by the primary and partner processing unit's execution of the safety program.

8. The safety controller of claim 7 wherein the safety program is executed repeatedly and wherein the synchronization program compares execution of the safety program at the conclusion of each repeated execution prior to outputting of the output values to the external device.

9. The safety controller of claim 1 wherein the safety program executes to generate values of internal variables and wherein the synchronization program compares execution of the safety program by comparing values of internal variables generated by the primary and partner processing units executing the safety program.

10. The safety controller of claim 1 wherein the safety program is executed repeatedly and wherein the synchronization program compares execution of the safety program at a period greater than the repetition period.

11. The safety controller of claim 1 wherein the primary processing unit includes only a single processor.

12. The safety controller of claim 1 wherein the primary processing unit includes at least two processors.

13. The safety controller of claim 12 wherein the processors of the primary processing unit share a common memory.

14. The safety controller of claim 12 wherein the processors of the primary processing unit have independent memories.

15. The safety controller of claim 12 wherein the first processor of the primary processing unit communicates with the first memory by a memory bus not directly accessible to the second processor of the partner processing unit but only accessible by the second processor through the first processor and wherein the second processor of the partner processing unit communicates with the second memory by a memory bus not directly accessible to the first processor of the primary processing unit but only accessible by the first processor through the second processor.

16. The safety controller of claim 1 wherein the primary processing unit includes a transfer program for receiving programs from a user and for loading safety programs in the first and second memory and loading standard program information only in the first memory.

17. The safety controller of claim 16 wherein the safety program holds an identification value indicating that it is a safety program.

18. The safety controller of claim 1 wherein the first memory also holds standard data used or generated by the standard program and safety data used or generated by the safety program and wherein the second memory holds the safety data used or generated by the safety program.

19. The safety controller of claim 1 wherein the second memory holds portions only of the standard data.

20. A safety controller system comprising:

a programming terminal executing a programming tool to:

(a) accept program instructions from a user describing the logical combination of input sensor data to produce output control data;

(b) collect the program instructions into tasks;

(c) identify the tasks as to one of a first and second level of reliability, the first level executable on a single processing unit only and the second level requiring execution in tandem on two processing units having an ability to compare execution

to determine a fault in either of the two processors and to then enter a safety state; and

a safety controller having at least two independent processing units executing a stored program to receive the tasks from the programming terminal and provide both the first and second processing units with tasks identified to the second level and provide the first processing unit only the tasks identified to the first level.

21. The safety controller system of claim 20 wherein the safety controller further executes the stored program to compare execution of the tasks identified to the second level to enter a safety state when this execution differs.

22. A safety controller kit comprising:

a first controller having a first housing attachable to a backplane to communicate with other components of a control system, the first controller accepting control programs requiring a first level of reliability;

a second controller having a second housing attachable to the backplane to communicate with the first controller, the second controller accepting control programs requiring a second level of reliability greater than the first level of reliability to execute the control programs in tandem with the first controller; and

wherein the first controller further only accepts programs of the second level of reliability when the second controller is in communication with the first controller over the backplane.

23. A method of operating a safety controller having primary and partner independent processing units comprising the steps of:

(a) receiving a safety program requiring a second reliability of operation and a standard program requiring a first reliability of operation less than the second reliability of operation;

(b) loading the safety program in the primary and partner processing units and executing the safety program in tandem in the primary and partner processing unit to enter a safety state when execution differs in the primary and partner processing units; and

(c) loading the standard program in the primary processing unit only and executing the standard program.

24. The method of claim 23 wherein the safety program executes to generate outputs to be used to control an external device and wherein step (b) compares execution of the safety program by comparing outputs generated by the primary and partner processing unit's execution of the safety program.

25. The method of claim 24 wherein the safety program is executed repeatedly and wherein step (b) compares execution of the safety program at the conclusion of each repeated execution prior to outputting of the output values to the external device.

26. The method of claim 24 wherein the safety program executes to generate values of internal variables and wherein step (b) compares execution of the safety program by comparing values of internal variables generated by the primary and partner processing units executing the safety program.

27. The method of claim 23 wherein the safety program is executed repeatedly and wherein step (b) compares at least some of the results of the execution of the safety program at a period greater than the repetition period.

28. The method of claim 23 wherein step (a) receives the standard program and the safety program at the primary processing unit only and transfer the safety program only to the partner processing unit.

29. The method of claim 28 wherein the safety program holds an identification value indicating that it is a safety program and step (a) identifies the safety program to be transferred by the identification value.

30. The method of claim 23 step (b) loads some standard data used or generated by the standard program to the partner processing unit.

31. A method of operating a safety controller system comprising the steps of:

(a) accepting program instructions from a user describing the logical combination of input sensor data to produce output control data;

(b) collecting the program instructions into logical tasks;

(c) identifying the task as to one of two levels of reliability, a first level executable on a single processor and a second level requiring execution in tandem on two processors having an ability to compare execution to determine a fault in either of the two processors and to then enter a safety state;

(d) executing the tasks identified to the first level of reliability on a first processor only; and

(e) execution of the task identified to the second level of reliability on the first and a second processor in tandem to identify processor faults.